

ORIGINAL

DOCKET FILE COPY ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

DEC 12 1997

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Communications Assistance for
Law Enforcement Act

)
)
)
)
)

CC Docket No. 97-213

**COMMENTS OF THE PERSONAL
COMMUNICATIONS INDUSTRY ASSOCIATION**

Eric W. DeSilva
Stephen J. Rosen
WILEY, REIN & FIELDING
1776 K Street, NW
Washington, DC 20006
(202) 429-7000

Mark J. Golden,
Senior Vice President, Industry Affairs
Mary E. Madigan,
Vice President, External Affairs
PERSONAL COMMUNICATIONS
INDUSTRY ASSOCIATION
500 Montgomery Street, Suite 700
Alexandria, VA 22314-1561
(703) 739-0300

December 12, 1997

No. of Copies rec'd
List ABCDE

026

Table of Contents

	Page
I. INTRODUCTION AND SUMMARY	2
II. THE COMMISSION SHOULD EXTEND CALEA'S COMPLIANCE DEADLINE ON A BLANKET BASIS UNTIL COMPLIANT EQUIPMENT IS AVAILABLE FROM EACH CARRIER'S REGULAR EQUIPMENT VENDOR.....	3
III. RESELLERS SHOULD BE INCLUDED WITHIN THE DEFINITION OF "TELECOMMUNICATIONS CARRIER" TO THE EXTENT NECESSARY TO ACCOMPLISH THE PURPOSES OF CALEA	6
IV. PRIOR TO PLACING NEW OBLIGATIONS ON PAGING PROVIDERS, THE COMMISSION SHOULD TAKE INTO ACCOUNT THE ADEQUACY OF PAGING PROVIDERS' CURRENT CAPABILITIES.....	8
V. THE RULES REGARDING SECURITY POLICIES SHOULD REDUCE THE ADMINISTRATIVE BURDENS ON BOTH LARGE AND SMALL CARRIERS	10
VI. CONCLUSION.....	13

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Communications Assistance for)	CC Docket No. 97-213
Law Enforcement Act)	
)	

**COMMENTS OF THE PERSONAL
COMMUNICATIONS INDUSTRY ASSOCIATION**

The Personal Communications Industry Association ("PCIA"),¹ by its attorneys, hereby submits its comments on the Commission's Notice of Proposed Rulemaking in the above-captioned proceeding.² As described in greater detail below, the Commission should, consistent with its statutory authority, take an aggressive role in ensuring that the Communications Assistance For Law Enforcement Act ("CALEA") is implemented in a manner that recognizes the economic and technical realities of the telecommunications industry.

¹ PCIA is the international trade association created to represent the interests of both the commercial and the private mobile radio service communications industries. PCIA's Federation of Councils includes: the Paging and Narrowband PCS Alliance, the Broadband PCS Alliance, the Site Owners and Managers Association, the Association of Wireless Communications Engineers and Technicians, the Private Systems Users Alliance, and the Mobile Wireless Communications Alliance. In addition, as the FCC-appointed frequency coordinator for the 450-512 MHz bands in the Business Radio Service, the 800 and 900 MHz Business Pools, the 800 MHz General Category frequencies for Business Eligibles and conventional SMR systems, and the 929 MHz paging frequencies, PCIA represents and serves the interests of tens of thousands of licensees.

² *Communications Assistance for Law Enforcement Act*, FCC 97-213 (Oct. 10, 1997) ("Notice").

I. INTRODUCTION AND SUMMARY

The Commission has been granted broad authority under CALEA to determine under what circumstances CALEA's compliance deadlines should be extended, define the meaning of "telecommunications carrier," thereby defining the scope of CALEA's requirements, and develop rules regarding carriers' security policies and procedures. The rules promulgated pursuant to this authority should reflect the business realities of the telecommunications industry as well as the technical limitations of currently available network equipment.

First, until CALEA-compliant equipment is available from carriers' regular equipment vendors, the Commission should utilize its Section 107(c) authority to issue blanket extensions of CALEA's compliance deadlines. Such blanket extensions are in the public interest because no carrier can adhere to the Section 103 assistance capability requirements until CALEA-compliant equipment is commercially available.

Second, resellers should be included within the definition of "telecommunications carrier" to the extent these entities have unique access to customer information that is essential to the expedient execution of electronic surveillance warrants. Because resellers have traditionally been classified as common carriers by the courts, and regulated as such by the Commission, treating them as "telecommunications carriers" for the purposes of CALEA would be consistent with prior practice. The Commission should not, however, require resellers to do the impossible by making resellers responsible for ensuring that the network of the underlying facilities-based carrier complies with CALEA's technical requirements.

Third, the Commission should be extremely cautious in imposing additional law enforcement related obligations on paging providers. Because paging providers currently offer

law enforcement officials adequate means of electronic surveillance, and will soon be required to enhance these capabilities, this caution is warranted.

Finally, the rules regarding carrier security policies and procedures should permit both large and small carriers to self-certify compliance. Because self-certification has proven successful and administratively efficient, including, for example, certifications in the highly sensitive area of the environmental effects of radiofrequency emissions, it is appropriate to use self-certification in the context of carrier security. Further, there are sufficient incentives, including the risk of loss of license, forfeitures, and civil suits, to ensure that carriers comply with the Commission's security policies and procedures.

II. THE COMMISSION SHOULD EXTEND CALEA'S COMPLIANCE DEADLINE ON A BLANKET BASIS UNTIL COMPLIANT EQUIPMENT IS AVAILABLE FROM EACH CARRIER'S REGULAR EQUIPMENT VENDOR

As a matter of law, under Section 107(c), the Commission, after consultation with the Attorney General, has the authority to extend the deadline for compliance with Section 103 "if compliance with the assistance capability requirements ... is not reasonably achievable through application of technology available within the compliance period."³ The October 25, 1998 deadline for compliance with the assistance capability requirements of Section 103 is rapidly approaching, and an interim technical standard has only recently been agreed upon by the Telecommunications Industry Association ("TIA").⁴ Therefore, upon petition by a carrier or trade association of carriers, the Commission should grant a blanket extension of the October 25,

³ 47 U.S.C. § 1006(c)(2).

⁴ TIA promulgated JStd 025 as an interim standard for CALEA-compliant
(Continued...)

1998 deadline for all carriers. Utilizing a blanket extension rather than individualized, carrier-by-carrier determinations is in the public interest because all carriers are similarly situated in lacking access to CALEA-compliant equipment.

Finally, the Commission seeks comment on the factors to be considered — in addition to those set forth in Section 109⁵ — in determining whether extensions of time to meet the assistance capability requirements should be granted under Section 107.⁶ Section 107 empowers the Commission to grant an extension of time if compliance with these assistance capability requirements is not “reasonably achievable through the application of technology available within the compliance period.”⁷ In determining whether such compliance is “reasonably achievable,” one additional factor that should be considered is the availability of CALEA-compliant equipment from a carrier’s regular equipment vendor.

(...Continued)

equipment. The standard is currently under review from ANSI.

⁵ Section 109(b)(1) describes a multi-factor test for determining whether compliance is “reasonably achievable.” These factors are: “(1) the effect on public safety and national security; (2) the effect on rates for basic residential telephone service; (3) the need to protect the privacy and security of communications not authorized to be intercepted; (4) the need to achieve the capability assistance requirements of section 103 by cost-effective methods; (5) the effect on the nature and cost of the equipment, facility, or service at issue; (6) the effect on the operation of the equipment, facility, or service at issue; (7) the policy of the United States to encourage the provision of new technologies and services to the public; (8) the financial resources of the telecommunications carrier; (9) the effect on competition in the provision of telecommunications services; (10) the extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995; and (11) such other factors as the Commission determines are appropriate.” 47 U.S.C. § 1008(b)(1).

⁶ Notice, ¶ 50.

⁷ 47 U.S.C. § 1006(c)(2).

Preliminarily, taking the availability of CALEA-compliant equipment into account in granting extensions is consistent with the plain meaning of “reasonably achievable through the application of technology available within the compliance period.”⁸ Under this standard, the Commission must determine whether a carrier can purchase, through normal distribution channels, the equipment it needs to bring its network into compliance with CALEA. In making this determination, the Commission should further examine whether the vendor from which the carrier normally procures its network equipment makes CALEA-compliant equipment available. Such an inquiry is essential because a carrier’s entire network is generally manufactured by a single vendor. Therefore, in order to meet CALEA’s requirements, unless that vendor manufactures CALEA-compliant equipment, a carrier might be required to replace a substantial portion of its capital plant to achieve compatibility with equipment from a third party, assuming such equipment is even available. The Commission’s rules on extensions should therefore be crafted to avoid such an inefficient and unfair result; a result not reasonably contemplated by Congress.

In addition, taking the availability of CALEA-compliant equipment into account in ruling on extensions is consistent with the statute’s intent in that the January 1, 1995 funding cutoff is premised on the prompt availability of equipment that meets the assistance capability requirements of Section 103. That is, in setting forth an installation or deployment date of January 1, 1995 as the date after which the Attorney General will no longer fund the retrofitting of a carrier’s equipment to bring it into compliance with CALEA, Congress must have implicitly

⁸ *Id.*

assumed that compliant equipment would be available shortly after that date.⁹ Otherwise, this deadline would merely be an arbitrary and capricious dividing line between carriers that would be fortunate enough to be reimbursed for bringing their equipment into compliance and those that would have to pay their own way. Thus, by adding this equipment availability factor to Section 109's multi-factor test, the Commission will harmonize its policy on extensions of the compliance deadlines with the overall structure and intent of CALEA.

III. RESELLERS SHOULD BE INCLUDED WITHIN THE DEFINITION OF "TELECOMMUNICATIONS CARRIER" TO THE EXTENT NECESSARY TO ACCOMPLISH THE PURPOSES OF CALEA

The Commission should include resellers within the definition of "telecommunications carrier" to the extent such a definition will further the aims of CALEA and is consistent with the Commission's long standing policy of regulating resellers as common carriers. As a matter of furthering the aims of CALEA, resellers, not the underlying facilities-based carrier, have access to the names, telephone numbers, and addresses of their end-user customers. Resellers usually have sole access to this customer information because the underlying carrier generally provides the reseller with blocks of telephone numbers and, at the end of every month, with call detail records for these numbers. The reseller, in turn, associates each number with a subscriber, provides resold services to that customer, and bills the customer. Thus, resellers are the only entities that can properly match the name and address of their customers with a telephone number.

⁹ See 47 U.S.C. §§ 1008(a), (d) (requiring the Attorney General to either pay carriers to make their pre-1995 equipment CALEA-compliant or deem the equipment to be in compliance).

Expedient access to such customer information is essential to the ability of carriers, pursuant to Section 103(a) of CALEA, to provide law enforcement officials with call content and call identifying information, and to associate that information with a specific “customer or subscriber.”¹⁰ Consequently, any failure to require resellers to comply with CALEA’s warrant execution requirements will create a significant gap in the ability of law enforcement agencies to engage in court authorized electronic surveillance.

Classifying resellers as common carriers for the purpose of satisfying surveillance warrants not only fulfills the goals of CALEA, but is also consistent with the manner in which the Commission and the courts have traditionally categorized resellers. As stated in the *Resale and Shared Use Order*, “an entity engaged in the resale of communications service is a common carrier, and is fully subject to the provisions of Title II of the Communications Act.”¹¹ Resellers, as telecommunications entities that hold themselves “out indiscriminately to the clientele [they are] suited to serve,”¹² and allow customers to “transmit intelligence of their own design and choosing,” also fall within the judicially sanctioned definition of “common carrier.”¹³ Thus, because resellers have already made the necessary adjustments to their business plans to function

¹⁰ 47 U.S.C. § 1002(a).

¹¹ *Regulatory Policies Concerning Resale and Shared Use of Common Carrier Services and Facilities*, 60 FCC 2d 261, ¶ 8 (1976).

¹² *National Association of Regulatory Utility Commissioners v. FCC*, 525 F.2d 630, 641 (D.C. Cir.), *cert. denied*, 425 U.S. 922 (1976) (“*NARUC I*”).

¹³ *National Association of Regulatory Utility Commissioners v. FCC*, 553 F.2d 601, 608 (D.C. Cir. 1976) (quoting *Industrial Radiolocation Service*, 5 FCC 2d 197, 202 (1966)) (“*NARUC II*”).

as regulated entities, subjecting them to certain requirements of CALEA will not represent a radical change.

Resellers should not, however, be responsible for ensuring that the network of the underlying facilities-based carrier complies with the assistance capability requirements of Section 103 or the capacity requirements of Section 104. Placing such a burden on resellers will not further the purposes of CALEA and is illogical, because the reseller has no control over the manner in which the network of the facilities-based carrier is configured. Thus, while resellers should be required to assist in the execution of electronic surveillance warrants, they should not be required to fulfill the technical capability portions of CALEA.

IV. PRIOR TO PLACING NEW OBLIGATIONS ON PAGING PROVIDERS, THE COMMISSION SHOULD TAKE INTO ACCOUNT THE ADEQUACY OF PAGING PROVIDERS' CURRENT CAPABILITIES

Section 101(8)(c)(ii) of CALEA¹⁴ affords the Commission, after consultation with the Attorney General, the flexibility to exempt certain classes or categories of telecommunications carriers from CALEA's requirements. In determining which, if any, of CALEA's requirements should apply to paging providers, the Commission and the Attorney General should bear in mind that the messaging industry has in the past, and continues to, make every effort to provide law enforcement officials with the ability to engage in court ordered electronic surveillance.

Specifically, at present, paging providers routinely cooperate with law enforcement officials by providing them, pursuant to a valid court order, with the CAP codes of specific pagers and with clone pagers with these CAP codes installed in them. These clone pagers allow

¹⁴ 47 U.S.C. § 1001(8)(c)(ii).

law enforcement officials to surreptitiously receive whatever messages the target of the electronic surveillance warrant is receiving on his or her pager, thereby satisfying the intent of CALEA to provide law enforcement officials with call content and call identifying information.¹⁵

Alternatively, once police have the CAP code of a suspect's pager, they can also utilize commercially available testing equipment (*e.g.*, "Hark Verifier," "Advanced Signal Signal Pro") to decode the content of pages being sent to the pager in question.¹⁶ Further, because all CMRS paging systems are interconnected with the public switched network, law enforcement officials can capture the pages intended for the subject of a warrant by executing a surveillance warrant on the appropriate interconnecting landline carrier.

Against this background, the Commission should be cautious in imposing additional law enforcement related obligations on paging carriers until such time as law enforcement officials state that the paging industry needs to implement further measures to satisfy CALEA related obligations. Such caution is warranted because practices already in place allow the court ordered electronic surveillance of paging customers. With the passage of the Clone Pager Authorization Act, the procedures will be further upgraded. Imposing redundant requirements on paging carriers will merely make it more difficult and expensive for such providers to carry out their

¹⁵ The Clone Pager Authorization Act of 1996, S. 170, 105th Cong. (1997), has been passed by the Senate and referred to the House of Representatives. This Act will clarify that paging providers are legally obligated to provide law enforcement officials, pursuant to a court order, with access to "clone pagers."

¹⁶ If law enforcement officials frequently monitor many pagers, purchasing commercially available test equipment may be less expensive and more convenient than cloning pagers.

business, without providing law enforcement officials with any more powerful weapons in their war against crime.

V. THE RULES REGARDING SECURITY POLICIES SHOULD REDUCE THE ADMINISTRATIVE BURDENS ON BOTH LARGE AND SMALL CARRIERS

In its *Notice*, the Commission proposes two distinct methods of monitoring carrier security policies and procedures pursuant to Section 229. Under this proposal, large carriers (*i.e.*, those with \$100,000,000 or more in indexed annual operating revenues), will be required to make individual filings “that contain detailed statements of the policies, processes, and procedures that each carrier will use to comply with the requirements that are imposed by CALEA.”¹⁷ Small carriers (*i.e.*, those with less than \$100,000,000 in indexed annual operating revenues), on the other hand, have the option of either filing a statement describing their security policies and procedures, or certifying that they observe procedures consistent with the Commission’s systems security rules.¹⁸

PCIA believes that all telecommunications carriers, both large and small, should be permitted to take advantage of the more streamlined monitoring procedures the Commission has proposed for small carriers. Such streamlined procedures are in the public interest because they reduce the administrative burden on all carriers, thereby increasing efficiency and minimizing customer rate impacts. Further, allowing carriers to self-certify avoids placing the FCC in the difficult position of micromanaging carriers’ internal policies.

¹⁷ *Notice*, ¶ 35.

¹⁸ *Id.*

These streamlined procedures will in no way compromise carrier implementation of the systems security and integrity provisions of Section 229. Critically, the Commission has already utilized self-certification in numerous other contexts, including ensuring that wireless facilities comply with the Commission's radiofrequency emissions requirements.¹⁹ Given its successful implementation in the highly sensitive health and safety context, there is no reason why such self-certification will not be similarly effective in the equally sensitive context of customer privacy.

Further, carriers that fail to comply with the Commission's policies on system security and integrity face the daunting possibilities of forfeitures, loss of licenses, and civil suits brought under 18 U.S.C. § 2520 by disgruntled customers. Given the magnitude of forfeitures that the Commission is empowered to assess against common carriers for violations of its rules²⁰ — to say nothing of the possibility of a loss of license — licensees would be extremely imprudent to skirt these rules. These adverse consequences for rule violators provide significant incentives for carriers to take their self-certification programs seriously.

When executing a surveillance warrant, the Commission should also recognize business realities by modifying its proposal requiring a carrier's employees to sign an affidavit *prior* to participating in a communications intercept. Specifically, if the carrier is served with a warrant that requires the rapid implementation of electronic surveillance, there will be no time to execute

¹⁹ 47 C.F.R. § 1.1307.

²⁰ See 47 U.S.C. § 503(b)(2)(B) (authorizing forfeitures of up to \$1,000,000 for “any single act or failure to act”).

the detailed affidavit that the Commission has proposed.²¹ In recognition of this fact, employees should be given the flexibility to execute affidavits within a *reasonable period of time after* carrying out the intercept. This modification will lessen the compliance burden on carriers while still meeting the Commission's goal of enhancing carrier security.

Finally, it is important that carriers be able to check the criminal records of their security personnel by submitting the fingerprints of these personnel to federal or local law enforcement officials. Because these security personnel will have access to confidential information that is of great value to criminal enterprises (*i.e.*, information regarding whose phones are being tapped and when), higher levels of employee pre-screening are essential. As a general rule private employers are unable to definitively ascertain whether their employees have criminal records. Therefore, it is imperative that carriers be permitted to carry out such background checks for the purposes of implementing carrier security policies. This enhanced vigilance is a necessary tool in the prevention of the "leakage" of highly sensitive information that could defeat the purpose of electronic surveillance.

²¹ Notice, ¶ 31 (proposing that each affidavit contain the following information: (1) the telephone number(s) or the circuit identification number(s) involved; (2) the name of each employee and officer who effected the interception and possessed information concerning its existence, and their respective positions within the telecommunications carrier; (3) the start date and time of the interception; (4) the stop date and time of the interception; (5) type of interception; (6) a copy or description of the written authorization of the employee and officer to participate in interception activity; and (7) a statement that the employee or officer will not disclose information about the interception to any person not properly authorized by statute or court order).

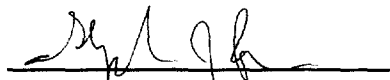
VI. CONCLUSION

The Commission has broad authority under CALEA to define terms, set forth carrier compliance regimens, and prescribe technical standards. This authority should be used in a manner that effectuates the goals of CALEA, recognizes the business and technical constraints within which telecommunications carriers operate, and does not arbitrarily discriminate against certain telecommunications carriers.

Respectfully submitted,

PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION

By:



Eric W. DeSilva
Stephen J. Rosen
WILEY, REIN & FIELDING
1776 K Street, NW
Washington, DC 20006
(202) 429-7000

By:



Mark J. Golden,
Senior Vice President, Industry Affairs
Mary E. Madigan,
Vice President, External Affairs
PERSONAL COMMUNICATIONS
INDUSTRY ASSOCIATION
500 Montgomery Street, Suite 700
Alexandria, VA 22314-1561
(703) 739-0300

December 12, 1997